International Journal of Computer Applications Technology and Research
Volume 5– Issue 3, 115 - 125, 2016, ISSN:- 2319–8656

Security Requirements and Security Threats In Layers Cloud and Security Issues Open Source Cloud

Roya Morshedi
Department of security
Information Engineering
Central branch
University of Malek ashtar
Tehran, Iran
Royamorshedi@gmail.com

Ali Payandeh
Department of Infrmation and
Communication Tecnology,ICT
Central branch
University of Malek ashtar
Tehran, Iran

Ali Pourghaffari
Department of Infrmation and
Communication Tecnology,ICT
Central branch
University of Malek ashtar
Tehran, Iran

Abstract: Euacalyptus, OpenNebula and Nimbus are three major open-source cloud-computing software platforms. The overall function of these systems is to manage the provisioning of virtual machines for a cloud providing infrastructure-as-a-service. These various open-source projects provide an important alternative for those who do not wish to use a commercially provide cloud. This is a fundamental concept in cloud computing, providing resources to deliver infrastructure as a service cloud customers, making users have to buy and maintain computing resources and storage. In other hand, cloud service providers to provide better resources and facilities customers need to know they are using cloud infrastructure services. In this end, we intend to security threats in the cloud layer and then to analyse the security services in cloud computing infrastructure as a service to pay.

Keywords: Infrastructure as a Service, Infrastructure as a Service security threats, security issues cloud computing infrastructure services

1. INTRODUCTION

Cloud computing infrastructure has unique properties compared to other layers of the source specification introduced new security risks to the community and security experts, industry practitioners and experts to find solutions appropriate security characteristics and risks of this new trend.Cloud computing is a relatively recent concept which combines technologies for resource management and provisioning with the ideas of mass deployment, elasticity and ease of use. To enterprises it is an interesting concept on several levels – from internal applications to the possibility of sharing resources with other organization or providing their own resources as a service to others. Predictions by IDC Adriatics suggests that 2011 will be a year of transition for the global cloud computing services as it is expected that the related technologies will graduate from the early adoption to the new mainstream phase [5]. Cloud computing has found significant support in the business world, with expected rises in the revenue coming from cloud-related services as high as 30%, public clouds valued at USD 29 billion, and private clouds valued at USD 13 billion. Predictions for more distant future are even more optimistic, with some predictions of its growth by 2014 being notably higher (as much as up to five times) than the average global IT spending, with a compound annual growth rate of 27%. Enterprises have a number of reasons to adopt cloud computing technologies among which are [4][10]: easier management of their resources, introduction of dynamic infrastructure, per-consumption billing, support for varied platforms and operating systems and the possibility to start and stop the provisioned resources as needed.

With the spread of computers, scientists are exploring ways to solve that increased computing power, processing power, resilience and optimal use of infrastructure, platforms and applications were discussed. The first scientific use of the term cloud computing was in an article in 1997. Amazon modernization of data centers, cloud computing has played a key role in the development and Eucalyptus in early 2008, the first open source platform for deploying private clouds became AWS- API compatible. In early 2008, OpenNebula, open source software for deploying private and hybrid clouds and for the federation of clouds. Despite all the benefits of this environment, there are security concerns in two main groups, security, cloud service providers and cloud customers are security issues. In this article we are going to discuss security issues in cloud infrastructure services.

2. CLOUD COMPUTING DEFINED

The basic concept of cloud computing and initiator Name of the 1950s, when large-scale mainframe computers in universities and companies through terminal was available. For efficient use of such processors, it is recommended that users can access these computers simultaneously from multiple terminals

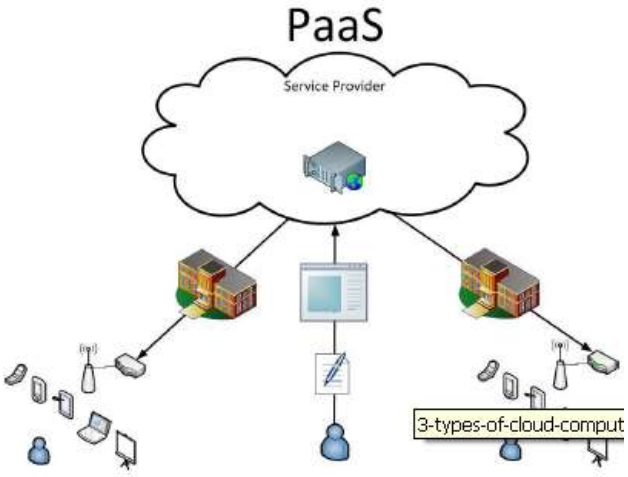
to share your information. With extensive computer scientists to explore solutions that enhance the computing power, processing power, high resilience and optimum use of infrastructure, platforms and applications were discussed. The first practical use of the term cloud computing in an article in 1997. Amazon modernization of data centers, cloud computing has played a key role in the development and Eucalyptus in early 2008, the first AWS- API compatible platform for deploying private clouds became open source. In early 2008, OpenNebula, open source software for deploying private and hybrid clouds as well as for the Federation of clouds.

They directly lead to introduction of the three common service models in which cloud computing is implemented [3]:

• *Software as a Service (SaaS)*, where the product is an application (usually a Web application) offered to users with little to no customizations. The users may have high-level administrative access to the application but have no control or influence on the application's implementation, inner workings or underlying infrastructure. This is an extension of the already popular hosted application model.

• *Platform as a Service (PaaS)*, where the product is a development and deployment platform, a set of APIs, libraries, programming languages and associated tools used for application creation. Users of PaaS are developers and companies which create

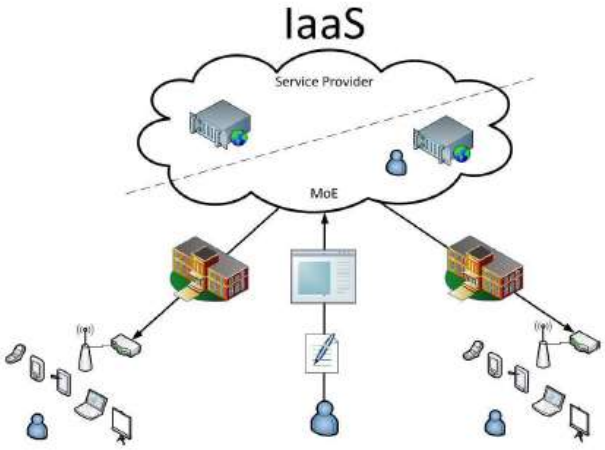
customized applications for end-users, and as such they are allowed to have control over some aspects of the application's environment but without direct access to the operating system and the hardware.



• *Infrastructure as a Service (IaaS)*, where the product is the low-level infrastructure used to create customized application environments or even higher level products (which might be PaaS or SaaS).

Users of IaaS are given complete control of their infrastructure resources (most notably, virtual machines) and can configure and use them as they see fit. IaaS is the lowest-level type of cloud service and it does not usually carry the obligation to use any prescribed technologies (though the hosted environments may be preconfigured).

These models progress from a high-level service model directly accessible to end-users to more low-level services in which their immediate users have control over the application or the basic infrastructure.



A. Cloud computing examples and target users Each of the models has its primary audience, its strengths and weaknesses. SaaS is already popular among endusers in the form of publicly available, widely used hosted applications like web-mail applications (e.g. Google Mail1, HotMail2, Yahoo Mail3), picture sharing applications (e.g. Picasa4, Flickr5), video clip sharing

applications (e.g. YouTube6, Vimeo7), and some forms of office applications (e.g. Google Apps8, Microsoft Exchange Hosted Services9, Microsoft Office Live10).

Such services are provided without giving users access to any advanced application, infrastructure or hardwarelevel configuration or management features. This benefits users who do not want to concern themselves with the technical aspects of the service, while allowing providers to reduce costs through mass deployments without significant reconfiguration and integration [6].

The PaaS model is oriented towards application developers and integrators, offering a common development and deployment platform for new applications or the customization of existing ones. It is successfully offered by Google (Google App Engine11),Microsoft (Windows Azure12) and Salesforce.com(Force.com13), among others. The model strongly focuses on developing applications that make use of the elasticity features offered by the platform, leaving lower-level tasks to the provider. As with the SaaS and the PaaS model, IaaS offers services to users, while removing a certain level of responsibility.

The users are given a larger degree of control over assigned resources, including storage, CPU and network resources, usually by allowing direct control of virtual machines. The properties of easy access, ondemand self-service and elasticity separate IaaS in cloud computing context from server hosting (and collocation) offered by a large number of companies. IaaS is implemented globally by providers such as Amazon(Amazon EC214), Rackspace (Rackspace Cloud15), FlexiAnt (FlexiScale16) and others. The IaaS model allows the greatest flexibility for users that can make use of it. It is the least complicated for providers, which need only concern themselves with the general infrastructure and running of the virtual machines, leaving users to manage the virtual machines' contents. Open source IaaS solutions suitable for enterprise use are the primary focus of this paper.

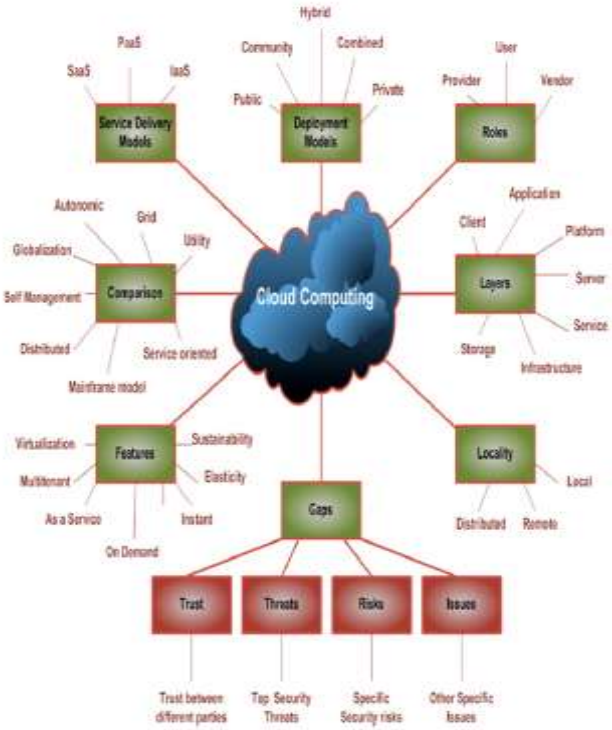


Fig. 1. Understanding cloud computing.[18]

3. *DEPLOYMENT MODELS*

The deployment models are orthogonal to the service models and describe the availability of the cloud deployments [3]. The three basic deployment models are:

• ***Private clouds***, used exclusively by one organization, usually operated internally by theorganization.

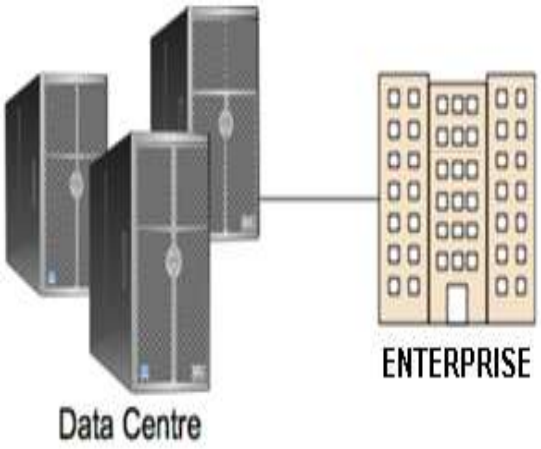
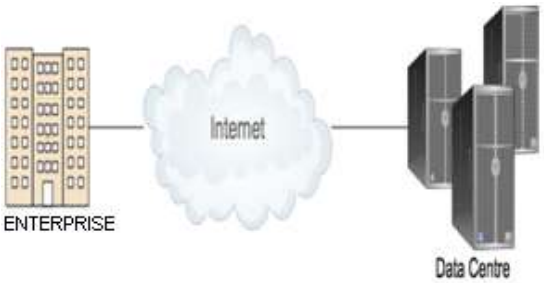


Fig2.privatecloud

• ***Public clouds***, used by generally interested parties(usually for a fee) in various ways. They can be



anextension of the "hosting provider" business model.

Fig3.public cloud

• ***Community clouds***, used by parties interested in specific requirements, such as organizations working on the same projects or on the sameproblem.

In addition to these three models, literature describes afourth model: a *hybrid cloud model* which combines two or more of the basic models. It is the most flexible model as it allows migrations of groups of resources between the categories.

In this work we focus on the *private cloud model* which can be used by enterprises to realize the benefits of cloud computing while still retaining control over the infrastructure they use [8][9].

4. Security Requirements In IaaS, PaaS, SaaS, [1]

There are already many existing laws and policies in place which disallow the sending of private data onto third-party systems. A Cloud Service Provider is another example of a third-party system, and organizations must apply the same rules in this case. It's already clear that organizations are concerned at the prospect of private data going to the Cloud. The Cloud Service Providers themselves recommend that if private data is sent onto their systems, it must be encrypted, removed, or redacted. Cloud computing is a service oriented Architecture which reduces information technology overhead for the end-user and provides great flexibility, reduced total cost of ownership ondemand services and many other benefits. Hence it delivers all IT related capabilities as services rather than product. Services on cloud are divided into three broad categories: software as a service, infrastructure as a service & platform as a service. Same as a service cloud is also classified as private cloud, public cloud & hybrid cloud.

Tabel 1. Security Requirements In IaaS, PaaS, SaaS

SaaS	PaaS	IaaS	Security Requirements
	✓	✓	Availability,resourcemanagement, trust, protection of communications, protection of the network and its resources, compliance, secure architecture, reliability and management of images
		✓	Control and governance, continuity of operations, risk management, protection of virtualization cloud, security hardware, hardware reliability, trusted third party, the basic configuration, the configuration change control, key management, connectivity to information systems, storage and computing
	✓		Identifying security threats, monitor configuration changes, procedures and security planning policy, accreditation, security, justice
✓		✓	Identity and Access Management
✓	✓		Anonymous

5. The Security Threats In The cloud layer

Because, the other two layer of service based on the cloud infrastructure layer are, security and management of cloud infrastructure services layer is very important security issues arise, storage facilities and processing services on a network as standard services We are, like server, switches, routers and so should be able to manage complex applications. other hand, cloud service providers to provide better resources to customers to use cloud computing services to make have.

The question then arises "How can the private data be automatically encrypted, removed, or redacted before sending it up to the Cloud Service Provider". It is known that encryption, in particular, is a CPU-intensive process which threatens to add significant latency to the

process. Large organizations using Cloud services face a dilemma. If they potentially have thousands of employees using Cloud services, must they create thousands of mirrored users on the Cloud platform? The ability to circumvent this requirement by providing single sign-on between on-premises systems and Cloud negates this requirement.

SaaS	PaaS	IaaS	Security threats	Row
×	√	√	Security threats	1
√	√	√	Insecure programming interfaces	2
×	×	√	Remove unsafe and incomplete data	3
×	×	√	Threats virtualization	4
√	√	√	Loss or data leakage	5
√	√	√	Hijacking Service	6
√	√	√	Personnel uncertain	7
√	√	√	Authorized change	8
√	√	√	Support research	9
√	√	√	Risk management interface	10
√	√	√	Traffic flow analysis	11
√	√	√	Connection failures and disruption of communication	12
×	×	√	Dependence secure hypervisor	13
×	×	√	Multitenant	14
√	√	√	Share issues related to technology and technology	15
√	√	√	Unknown risk profile	16
√	√	√	Attract hackers	17

Tabel 2.The Security Threats In The cloud layer [18]

6. OPEN SOURCE CLOUD COMPUTING PRODUCTS

We have selected a number of open source products which we consider to have a viable future for applications in enterprise environments. We intended to include the Enomaly ECP Community Edition17 but due to discontinuous work, we decided to omit it.

A. OpenNebula

OpenNebula18 is an open source software toolkit for cloud computing, which can be used to build and manage private, public and hybrid clouds. Since it does not contain virtualization, network, storage or security technologies, its primary use is as an orchestration tool for virtual infrastructure management in data-centers or clusters in private clouds and as merger of local and

public cloud infrastructure supporting hybrid scalable cloud environments.

Some of the main principles which guided the design of OpenNebula are full openness of architecture and interfaces, adaptability to various hardware and software combinations, interoperability, portability, integration, stability, scalability and standardization. Its main features include data-center or cluster management with Xen, KVM or VMware virtualization. It leverages the most common cloud interfaces Amazon AWS, OGF OCCI and VMware vCloud, and provides user management with authentication, multiple user rolling, secure multi-tenancy

and quota management. In the scope of cloud management a rich set of storage, virtual image, virtual machine and virtual network management features is provided. It supports cloud-bursting with Amazon EC2, simultaneous access to multiple clouds, and cloud federation. Standardization and interoperability are supported through abstraction from infrastructure and modular approach. Standard APIs includes Ruby, Java and XMLRPC. Security concerns are addressed with internal and external SSL communication and LDAP integration. OpenNebula EcoSystem adds a set of tools, extensions and plugins to OpenNebula Cloud Toolkit componentsenabling integration with existing products, services and management tools for virtualization, clouds and data centers. Telecom and hosting market,

and respectable scientific organizations like CERN adopted OpenNebula.

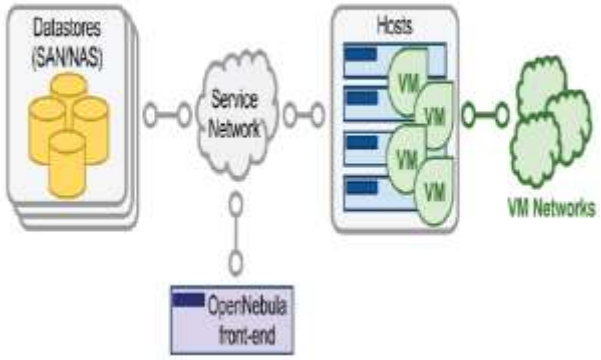


Fig4.Opennebula

B. Eucalyptus

As you can see, Eucalyptus composed of different elements, such as the cloud controller, cluster controller, storage controller, SC and NC have been formed.Cloud controller through a Web interface that provides the user the possibility to gain your virtual machine. Infrastructure also interacts with internal components. Storage controller acts as a storage system to protect files and virtual machine images. This component, such as a storage tank controller is permanent and stable. Information and samples of reservoir controller also makes maintenance and protection. Cloud controller and controller nodes associated with the cluster controller and task management and send commands to run on the controller node is responsible for the samples. Each cluster controller might consist of one or more controller nodes that all components monitor and manage them. In fact, the information received from the nodes to the cloud controller. Node controller, a machine that is installed Fvqnazr and do arithmetic operations. Also, the implementation, control and remove virtual machines on the Dard.kntrlknndh node by sending a query to the operating system, the amount of resources available, including the number of CPU cores, the RAM memory and disk space acquire this information to the cluster controller sends.Open source cloud computing architecture Eucalyptus[12] provides a scalable IaaS framework forimplementation of private and hybrid clouds. It wasinitially developed to support high performance computing (HPC) research at the University of California, Santa Barbara, and engineered to ensure compatibility with existing Linux-based data centers. It is component-based, flexible and highly modular with welldefined interfaces. Main design goals were simple

installation, non-intrusion and standardized language-independent communication. Eucalyptus also provides avirtual network overlay that isolates user network traffic and allows multiple clusters to appear as in the same LAN. Eucalyptus implements the Amazon Web Service (AWS) API allowing interoperability with existing services, enabling the possibility to combine resources from internal private clouds and from external public clouds to create hybrid clouds. This capability presents seamless integration with Amazon EC2 and S3 public cloud services. Eucalyptus currently supports Xen and KVM virtualizations, with plans to support others.

Four high level components are implemented as Web services. Cloud Controller (CLC) is a set of resource, data and interface services used for managing resources via node manager's queries, scheduling and cluster controller requests, visible as the main user interface. Storage Controller (Walrus) is a data storage service compatible with Amazon's S3 interface and Web services REST and SOAP interfaces. It accesses and stores virtual machine images and user data. Node Controller (NC) controls the execution, resources availability, and authorization on the host node. Cluster Controller (CC) collects information about a set of NCs, schedules run requests to NCs, and controls the instance virtual network overlay. Eucalyptus can be deployed on all major Linux OS distributions, including Ubuntu, Red Hat Enterprise Linux, CentOS, openSUSE, and Debian. Eucalyptus software core is included in Ubuntu distributions as a key component of the Ubuntu Enterprise Cloud.

According to [Nurmi et al 2009], the Eucalyptus project presents four characteristics that

differentiate it from others cloud computing solutions: a) Eucalyptus was designed to be simple without requiring dedicated resources; b) Eucalyptus was designed to encourage third-party extensions through modular software framework and language-agnostic communication mechanisms; c) Eucalyptus external interface is based on the Amazon API (Amazon EC2) and d) Eucalyptus provides a virtual network overlay that both isolates network traffic of different users and

allows clusters to appear to be part of the same local network.The Eucalyptus architecture is hierarchical and made up of four high level components, where each one is implemented as a stand-alone web service.

Node Controller (NC): this component runs on every node that is destined for hosting VM

instances. An NC is responsible to query and control the system software (operating system and hypervisor) and for conforming requests from its respective Cluster Controller. The role of NC queries is to collect essential information, such as the node's physical resources (e.g. the number of cores and the available disk space) and the state of VM instances on the nodes. NC sends this information to its Cluster Controller (CC). NC is also responsible for assisting CC to control VM instances on a node, verifying the authorization, confirming resources availability and executing the request with the hypervisor.

Cluster Controller (CC): this component generally executes on a cluster front¬end machine, or any machine that has network connectivity to two nodes:

one running NCs and another running the Cloud Controller (CLC). A CC is responsible to collect/report information about and schedule VM execution on specific NCs and to manage virtual instance network overlay.

Storage Controller (Walrus): this component is a data storage service that provides a mechanism for storing and accessing virtual machine images and user data. Walrus is based on web services technologies and compatible with Amazon's Simple Storage Service (S3) interface [Amazon 2006].

Cloud Controller (CLC): this component is the entry-point into the cloud for users. Its main goal is to offer and manage the Eucalyptus underlying virtualized resources. CLC is responsible for querying node managers for resources' information, making scheduling decisions, and implementing them by requests to CC. This component is composed by a set of web services which can be grouped into three categories, according their roles: resource services, data services, and interface services. While the details of the underlying resource architectures on which these systems operate are not commonly published, EUCALYPTUS is almost certainly shares some architectural features with these systems due to shared objectives and design goals. In addition to the commercial cloud computing offerings mentioned above (Amazon EC2/S3, Google AppEngine, Salesforce.com, etc.), which maintain a proprietary infrastructure with open interfaces, there are opensource projects aimed at resource provisioning with the help of virtualization.

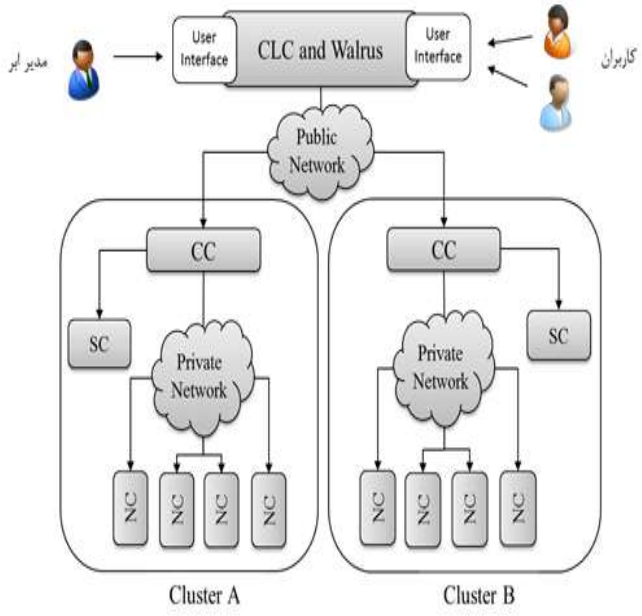


Fig5. Eucalyptus

Canonical's Ubuntu Linux distribution presents itself as a cloud OS with several cloud strategies, two of which are IaaS. Ubuntu Server Edition enables the use of Amazons EC2 but only as a public cloud. Ubuntu Enterprise Cloud (UEC)19 integrates Ubuntu Server Edition with

Eucalyptus over KVM hypervisor. The infrastructure of UEC is similar to Amazon's, but with simpler creation of private clouds.UEC [13] exposes five high-level components in a form of Web services: Cloud Controller (CLC), Walrus Storage Controller (WS3), Cluster Controller (CC), Node Controller (NC), and Elastic Block Storage Controller (EBS). The first four have the same functionalities as described in Eucalyptus overview, EBS runs besides CLC and provides persistent block devices and point-in-time volume snapshots stored on WS3. UEC defines security layers for authentication and authorization, network isolation, and machine instance isolation. Network isolation can be performed in four networking modes: system, static, managed and managed-noVLAN. Machine instance isolation is provided on three levels: networking, OS, and hypervisor-based machine.

D. OpenQRM

OpenQRM20 advertises itself as a data-center management platform. The core of openQRM follows the modern modular design and has no functionality itself, but instead focuses on abstracting storage and resources (computing resources, running virtual machines, VM images and other objects). OpenQRM features are provided via plugins which use the services exposed by the openQRM base. This architecture aims to make the whole system more stable and easier to manage as the base changes less often and provides a solid platform. OpenQRM can be installed on a variety of officially supported Linux operating systems: Debian, Ubuntu, SuSE, CentOS and Fedora. To achieve its goal of managed virtualized data-center, openQRM provides server and storage management, high-availability, realtime monitoring and virtual machine deployment and provisioning services, among others.

OpenQRM plugins provide a wide range of services, from integrated storage management (supporting directattached storage, and various SAN and NAS variants: iSCSI, LVM2, ATA-over-Ethernet and NFS), abstraction of virtualization (Xen, KVM, Linux-VServer, VMware Server and ESX VMs), migration from physical to virtual machines in three combinations (P2V, V2P and V2V of different VM type), high-availability (with failover from physical to virtual machines, and virtual to virtual failover between machines of same, or different type), and VM image templates or appliances.

E. Abiquo

Abiquo21 is a cloud management solution for virtualized environments in open source and commercial versions, mainly differing in resource limits, management and support options. Open source Abiquo Community Edition is licensed under LGPL Version 3. Main features include multi-tenancy, hierarchical user management and role based permissions with delegated control, resource limits, network, storage and workload management, multiple public, shared and private image libraries. It supports many Linux distributions (Red Hat, OpenSUSE, Ubuntu, Debian, CentOS, and Fedora), Oracle OpenSolaris, Microsoft Windows, and Mac OS X. Abiquo uses two storage systems: Appliances repository for virtual images in the form of NFS shared folder, and Virtual storage for virtual block devices available only in Enterprise edition. It distinguishes several types of server-side services: Java EE compatible application servers, database servers, cloud node servers, Appliance repository servers, and ISC DHCP servers. REST API can be used for integration with other systems. Abiquo server node incorporates Abiquo Core which contains the business logic, Appliance Manager for image library management and BPM that executes complex asynchronous tasks. Remote services deployed in the cloud expose system monitoring and management of virtual resources, physical machines, and storage.

Abiquo supports various virtualization technologiesincluding VMware ESX and ESXi, Hyper-V, VirtualBox,Xen, Citrix XenServer and KVM. Users of this solution benefit from powerful web management with functionalities such as drag-and-drop service deployment. It can be used for private clouds but also provides support for Amazon EC2. *F. Red Hat Cloud Foundations, Edition One* Red Hat22 offers a suite of open source software which provides infrastructure for public and private cloud solutions [11]. Red Hat Cloud Foundations, Edition One (RHCF) comprises of a set of products for virtualization, cloud, and application management and scheduling, but also operating systems, middleware, cookbooks, reference architectures with deployment instructions, consulting services, and training. RHCF Products are often tightly coupled with other Red Hat products. The suite comprises of Red Hat Enterprise Virtualization (RHEV), Red Hat Enterprise Linux (RHEL), Red Hat Network (RHN) Satellite, Red Hat Cluster Suite (RHCS), and Red Hat Enterprise MRG. RHEV for Servers is a product for end-to-end virtualization consisting of two components: RHEV Manager (RHEV-M) as a server virtualization system that provides advanced features (high availability, live migration, storage management, scheduler, etc.), and RHEV Hypervisor (RHEV-H), based on KVM hypervisor and deployed standalone or as RHEL hypervisor. RHN Satellite is a system management product providing software updates, configuration management, provisioning and monitoring across physical and virtual RHEL servers. RHCS is a clustering solution for RHEL supporting application/service failover and IP load balancing. Red Hat Enterprise MRG is a high-performance distributed computing platform providing messaging (MRG Messaging), real-time (MRG Realtime) and grid (MRG Grid) functionalities, and support for distributed tasks. Red Hat is investing and strongly participating in several cloud computing-related open source projects: Deltacloud, BoxGrinder, Cobbler, Condor, CoolingTower, Hail, Infinispan, Libvirt, Spice, and Thincrust. Red Hat also delivers JBoss Enterprise Middleware as a PaaS solution.

G. OpenStack

Collaborative software project OpenStack23, intends to produce an ubiquitous open source cloud computing platform that will meet the needs of public and private clouds regardless of size, at the same time be simple to implement and massively scalable.

Three interrelated components are currently under development: OpenStack Object Storage used for creation of redundant and scalable storage using clusters of commodity servers, OpenStack Imaging Service for retrieval of virtual machine images, and OpenStack Compute for provisioning and management of large groups of virtual private servers. OpenStack Compute represents cloud computing fabric controller and orchestrator for IaaS platform which can be used for management of various resources, networking, security, and access options. It defines drivers that interact with underlying virtualization mechanisms running on host and exposes functionality over a web-based API, but does not include any virtualization software. It is comparable to Amazon EC2 with additional support for projects that include volumes, instances, images, VLANs, keys and users. Images management relies on euca2ools (provided by Eucalyptus) and images are served through OpenStack Imaging Service or OpenStack Compute Service, supporting Amazon S3, OpenStack Object Storage or local storage. It also supports several virtualization standards including KVM, UML, XEN, Hyper-V and QEMU. OpenStack Compute can be deployed on Ubuntu, with tests on CentOS and RHEL under way.[23]

Fig6.Openstack

H. Nimbus

Nimbus24 is a set of open source software cloud computing components written in Java and Python targeting the needs of the scientific community, but also supporting other business use-cases. The main component is the Workspace service which represents a standalone site VM manager with different remote protocol frontends, currently supporting Nimbus WSRF frontend and partially Amazon EC2 with SOAP and REST interface. While Workspace service represents a compute cloud, there is also a quota-based storage cloud solution Cumulus, designed to address scalability and multiple storage cloud configurations. There are two types of clients: cloud clients for quick instance launch from various sites, and reference clients acting as full command-line WSRF frontend clients. Context Broker service allows clients to coordinate large virtual cluster launches using Context Agent, a lightweight agent on each VM. Context Broker manages a common cloud configuration in secure context across resources provisioned from potentially multiple clouds, with a possibility to scale hybrid clouds across multiple distributed providers. Nimbus supports the Xen or KVM hypervisors, and virtual machine schedulers Portable Batch System and Oracle Grid Engine The main advantage of Nimbus compared to OpenNebula is that it exposes EC2 and WSRF remote interfaces with attention to security issues, and can be combined with OpenNebula VM manager.

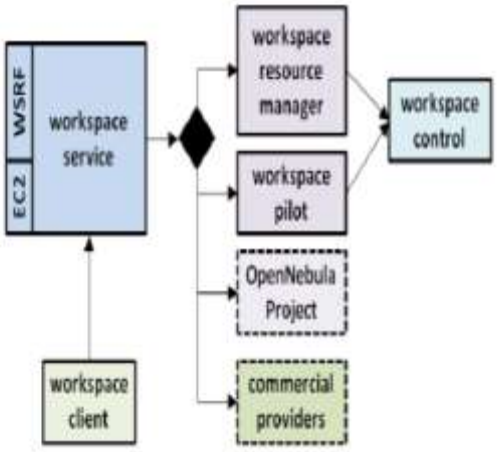


Fig7.Nimbus

I. mOSAIC

The main goal of the mOSAIC project [14] is the design of open source language- and platform independent API for resources and usage patterns that could be used in multiple cloud environments and construction of open source portable platform for cloud services. At the

current time there are no software deliverables, but the work is ongoing in cloud ontology, API description, testing environment, and usage patterns.

7. EVALUATION CRITERIA

Evaluating open source cloud computing products requires an elaborate set of evaluation criteria in order to provide a common baseline for IaaS cloud comparison. We have devised a set of 95 criteria which target features interesting for enterprise deployment. The criteria are grouped into six main categories: storage, virtualization, management, network, security and support. Storage-related criteria focus on supported approaches to storage: direct-attached storage, storage area network, and network-attached storage, as well as support for backup technologies and storage types. Virtualization criteria include virtualization types, support for actual virtualization technologies, and various monitoring and reconfiguration features, as well as support for migration and provisioning. Management features are essential for cloud implementers. The related criteria group captures features such as hardware and software integration, accounting, mass maintenance, reporting, and recovery.

Network features are highly dependent on the actual implementation, and the criteria focus on VLAN, firewall, performance, and integration support. Security criteria deal with permission granularity, integration with various directories, auditing, reporting of security events. Additional important features include storage encryption and secure management access.

OEM support is vital for enterprise deployment, and related criteria include an estimate of community vitality, vendor track record, possible support channels and SLAs, future viability of the product ecosystem, and completeness of provided free releases of the product.The criteria were devised with open source IaaS products in mind, but can be easily expanded to include commercial/closed technologies.

8. CONCLUSION AND FUTURE WORK

the solution presented And. these challenges, this area has become an important issue and the subject of security in cloud infrastructure services arise, the need for security among all levels of the cloud, most felt at the level of infrastructure as a service. becaus needs such as avaiability, reliability, data integrity, recovery, privacy and auditing in these areas become more tangible.

9. REFERENCES

[1] F. B. Shaikh, S. Haider, **"Security Threats in Cloud Computing"**, IEEE Internet technology and Secured Transactions (ICITST), 2011, pp 241-219.

[2] A.Bouayad et al, **"Cloud Computing: Security Challenges"**, IEEE Computer Knowledge and Technology 24, 2012, pp 26-31.

[3] I. Iankoulova, M. Daneva, **"Cloud Computing Security Requirements: a Systematic Review"**, Research Challenges in Information Science (RCIS) IEEE, 2012, pp 1 - 7.

[4] Dawoud, Wesam, Takouna, Ibrahim, Meinel, Christoph,**Infrastructure as a service security: Challenges and solutions**, Informatics and Systems (INFOS), 2010 The 7th International Conference onYear: 2010

[5] Djenna, Amir, Batouche, Mohamed,**Security problems in cloud infrastructure**,Networks, Computers and Communications, The 2014 International Symposium on year:2014,pp1-7.

[6] Hay, Brian, Nance, Kara, Bishop, Matt,**Storm Clouds Rising: Security Challenges for IaaS Cloud Computing**,System Sciences (HICSS), 2011 44th Hawaii International Conference on ,Year: 2011,PP:1-7,DOI: 10.1109/HICSS.2011.386.

[7] Chavan, Pragati, Patil, Premajyothi, Kulkarni, Gaurav, Sutar, R., Belsare, S,**IaaS Cloud Security**, Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on, Year: 2013 ,PP: 549 - 553, DOI: 10.1109/ICMIRA.2013.115

[8] Kumar, Saroj, Singh, Priya, Siddiqui, Shadab,**Cloud security based on IaaS model prospective**, Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference onYear: 2015,PP: 2173 – 2178.

[9] Winai Wongthai, Rocha, F., Van Moorsel, Aad,**Logging Solutions to Mitigate Risks Associated with Threats in Infrastructure as a Service Cloud**,Cloud Computing and Big Data (CloudCom-Asia), 2013 International Conference onYear: 2013 PP: 163 - 170, DOI: 10.1109/CLOUDCOM-ASIA.2013.70.

[10] Ristov, Sasko, Gusev, Marjan,**Security evaluation of open source clouds**,EUROCON, 2013 IEEEYear: 2013, PP: 73 - 80, DOI: 10.1109/EUROCON.2013.6624968.

[11] Litvinski, Oleg, Gherbi, Abdelouahed,**Openstack scheduler evaluation using design of experiment approach**,Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), 2013 IEEE 16th International Symposium onYear: 2013 ,pp: 1 - 7, DOI: 10.1109/ISORC.2013.6913212.

[12] P. Sempolinski and D. Thain, **"A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus"**, IEEE In Cloud Computing Technology and Science (CloudCom), 2010, pp 417-425.

[13] Donevski, A., Ristov, S., Gusev, M.,**Securityassessment of virtualmachines in opensourceclouds**, Information & Communication Technology Electronics & Microelectronics , (MIPRO), 2013 36th International Convention on, Year: 2013 PP: 1094 – 1099.

[14] Ristov, Sasko, Gusev, Marjan, Donevski, Aleksandar,**Security Vulnerability Assessment of OpenStack Cloud**,Computational Intelligence, Communication Systems and Networks (CICSyN), 2014 Sixth International Conference onYear: 2014 ,PP: 95 - 100, DOI: 10.1109/CICSyN.2014.32

[15] Haddad, Sammy, Dubus, Samuel, Hecker, Artur, Kanstrén, Teemu, Marquet, Bertrand, Savola, Reijo,**Operational security assurance evaluation in open infrastructures**,EUROCON, 2013 IEEE, PP:73 - 80 , DOI:10.1109/EUROCON.2013.6624968 .

[16] Achuthan, Krishnashree, SudhaRavi, Sreekutty, Kumar, Ravindra, Raman, Raghu, **Security vulnerabilities in open source projects: An India perspective**,Information and Communication Technology (ICoICT), 2014 2nd International Conference onYear: 2014 PP: 18 - 23, DOI: 10.1109/ICoICT.2014.6914033

[17] Bee Bee Chua, Bernardo, Danilo Valeros, **Open Source Developer Download Tiers: A Survival Framework**,IT Convergence and Security (ICITCS), 2013 International Conference on Year: 2013 PP: 1 - 5, DOI: 10.1109/ICITCS.2013.6717864

[18] Md.T.Khorshed, A.B.M.Shawkat, S. A.Wasimi,**"A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Iass"**, Journal of Future Generation Computer Systems, 2012, 833–85

[19] M.Asadullah, R.K.Choudhary, **"Data Outsourcing Security Issues and Introduction of DOSaaS in Cloud Computing"**, International Journal of Computer Applications (0975 – 8887) Volume 85 – No 18, January 2014, pp 40-44.

[20] N.Uma, **"Nelson, Semantic Based Resource Provisioning and Scheduling in Interlude Environment,"** Mobilizing resources in Latin America: The political economy of tax reform in Chile and Argentina. Palgrave Macmillan, 2012.

[21] K.Wood, M.Anderson, **"Understanding the Complexity Surrounding Multi tenancy in Cloud Computing",** IEEE Understanding the complexity surrounding multitenancy in cloud computing In e-Business Engineering (ICEBE), 2011, pp119-124.

[22] A. Abdullah, **"Resource Gate: A New Solution for Cloud Computing Resource Allocation"**, International Journal of Engineering and Technology Volume 2 No. 12, December, 2012

[23] http://www.OpenStack.org

[24] S. Ristov, et al, **"OpenStack Cloud Security Vulnerabilities from Inside and Outside"**, In CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 101-107. 2013

[25] http://archives.opennebula.org/documentation:rel4.4:plan

[26] Oliver Popović1et al, **"A Comparison and Security Analysis of the Cloud Computing Software Platforms"**, IEEE In Information Science and Engineering (ISISE), 2011, pp 632-634.

[27] Aleksandar Donevski, Sasko Ristov and Marjan Gusev, **Nessus or Metasploit: Security Assessment of OpenStack Cloud**,The 10th Conference for Informatics and Information Technology (CIIT 2013).